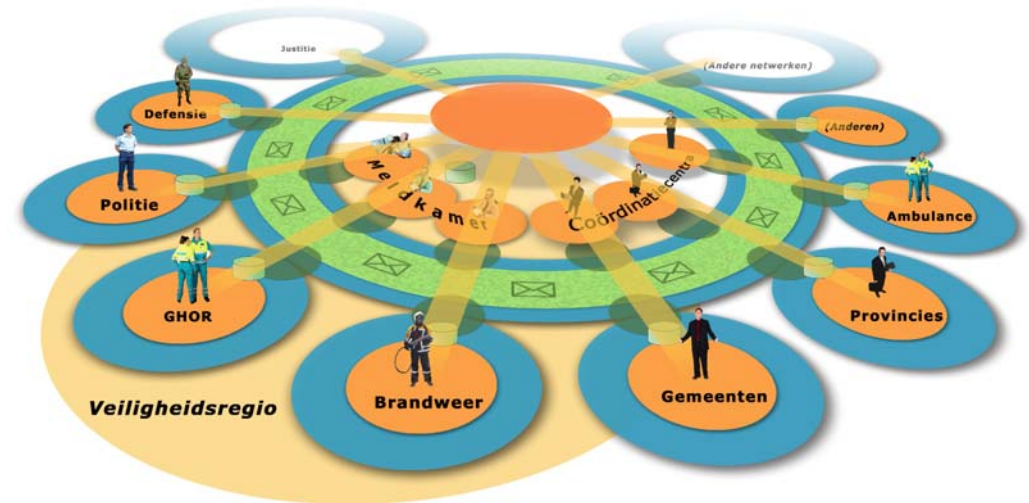


# Het Informatiebeleid Veiligheid

## *Verbinding in veiligheid*

---



# Het Informatiebeleid Veiligheid: *Verbinding in veiligheid*

---



# Het probleem

---

## Verskillende systemen voor de informatievoorziening die niet op elkaar aansluiten

Burgers, bestuurders en professionals moeten onder alle omstandigheden zo snel mogelijk de juiste informatie hebben om effectief op te kunnen treden bij een incident. Uit tal van evaluaties van rampen, crisis en rampenoefeningen als Voyager en Bonfire blijkt echter dat het zover nog niet is. Burgers willen dat de overheid bij een calamiteit snel en effectief optreedt. Informatievoorziening speelt hierin een essentiële rol. Voorsnog kenmerkt de informatievoorziening zich echter door een gebrek aan samenhang. Zowel op landelijk, regionaal en lokaal niveau zijn initiatieven gestart voor verbetering van informatievoorziening. Hieronder is dit geïllustreerd. Echter door deze versnippering, ontstaat een “bouwwerk” van onderdelen die niet goed op elkaar aansluiten en kunnen samenwerken. Hieronder is dit geïllustreerd.



# Het informatiebeleid Veiligheid

---

Het hebben en verkrijgen van informatie is van cruciaal belang voor alle veiligheidspartners (o.a. politie, brandweer, GHOR, gemeenten, waterschappen, defensie, maar ook burgers en bedrijven). Het klinkt simpel en logisch; U moet op het juiste moment, op de juiste plaats over de juiste informatie kunnen beschikken om effectief, efficiënt, gezamenlijk en individueel op te kunnen treden.

Het verbeteren van de informatievoorziening is een complex proces. Er zijn veel schakels in de veiligheidsketen die bovendien verschillen in cultuur, financiering, samenwerking en ICT-ontwikkeling. Ook is er soms sprake van een spanningsveld tussen eigen en gezamenlijke doelen. Het Ministerie van BZK wil dat de informatievoorziening verbeterd wordt, zowel binnen als tussen de kolommen. Hiertoe is een overkoepelende beleidsvisie ontwikkeld: het Informatiebeleid Veiligheid (IBV).

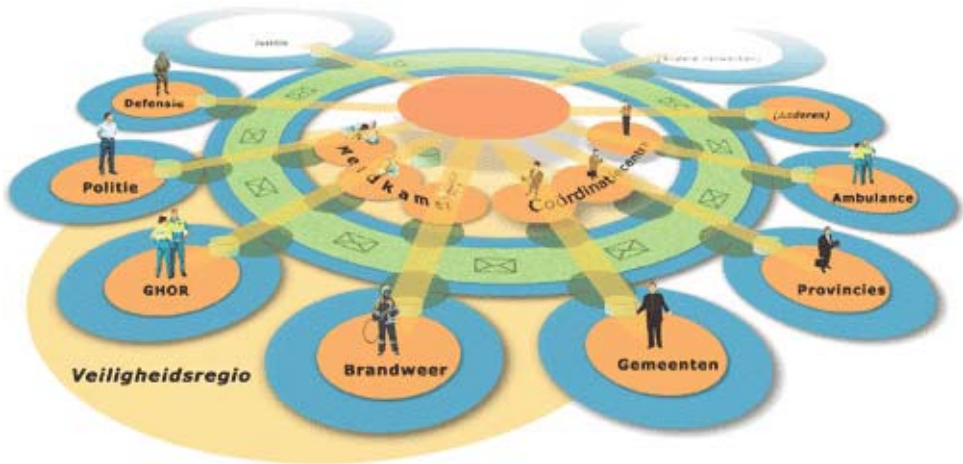
Dit beleid staat voor het verbeteren van het hebben en delen van informatie tussen de veiligheidspartners. Waar het om gaat is dat U de noodzakelijke en actuele veiligheidsinformatie deelt met elkaar. Zowel bij het normale optreden als in geval van een crisis of ramp. Het IBV leidt hiermee bij calamiteiten tot:

- goed geïnformeerde hulpverleners
- snellere responstijden
- een gezamenlijk situatiebeeld voor alle betrokkenen
- duidelijke communicatie
- snellere hulp
- goedkoop.

Het IBV levert daarmee een grote bijdrage aan het verhogen van uw presterend vermogen.

# Het Informatiebeleid Veiligheid - Verbindingen in Veiligheid

Het IBV gedachtegoed is samengevat in een model; het zogenaamde Galaxy model. Het model beschrijft dat er bestuurlijke afspraken er zouden moeten zijn (oranje), dat er verschillende soorten informatie gedeeld en herbruikt moeten worden (groen) en dat technische standaarden gehanteerd zouden moeten worden (blauw).



**Kaders en afspraken**  
over informatievoorziening  
zijn nodig tussen partijen:  
beleidsmakers, uitvoerders,  
regio's en leveranciers.

**Informatiestromen**  
Het hebben en delen van  
informatie met standaarden  
en onder architectuur

**Technologie**  
ICT basisvoorzieningen  
om gegevensontsluiting  
en gegevensuitwisseling  
adequaat te faciliteren

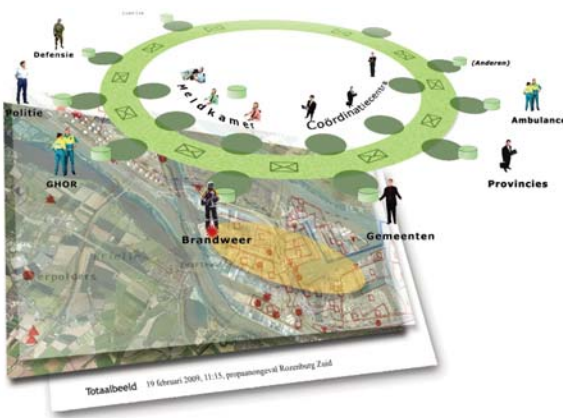
In deze Galaxy worden de vele lopende en in ontwikkeling zijnde activiteiten in beeld gebracht. Deze lopende activiteiten moeten het gezamenlijk mogelijk maken dat u voldoende informatie krijgt en uitwisselt.

# De doelen van het Informatiebeleid Veiligheid

---

Om tot uitvoerbaar beleid te komen zijn missie en visie vertaald in vier strategische **doelen**

- 1 **Beter;** verbeteren prestatievermogen van de Veiligheidssector door de juiste informatie op de juiste tijd bij de juiste gebruiker te krijgen;
- 2 **Robuust;** informatievoorzieningen robuust juist bij rampen en crises; informatie-uitwisseling en communicatie mogen dan niet uitvallen
- 3 **Beheersbaar;** (ICT voorzieningen) implementeren in kleinere delen (modules); geen grand designs, grote masterplannen of grote ICT-systemen die nauwelijks te beheersen zijn;
- 4 **Goedkoper;** gezamenlijk gebruik van informatievoorzieningen; niet steeds het wiel opnieuw uitvinden, maak gebruik van wat anderen al hebben ontwikkeld, eventueel door ze aan te passen aan de eigen situatie i.p.v. ieder voor zich alle zelf te ontwikkelen.



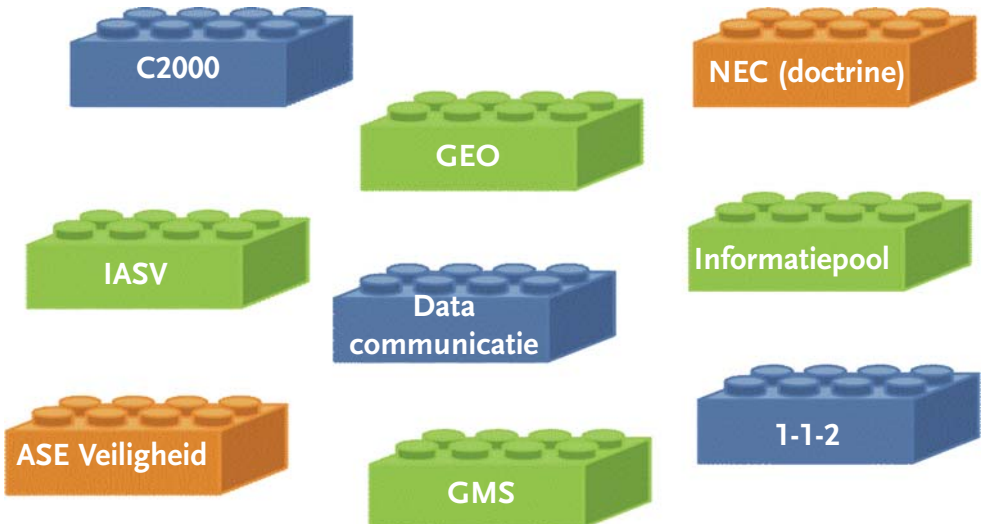
*U ziet een totaalbeeld van een getroffen gebied. Verschillende spelers uit het veiligheidsdomein zullen in actie moeten komen en gebruik maken van elkaars informatie. De groene ring uit de Galaxy geeft aan welke informatie met elkaar gedeeld moet worden. Waarbij het van belang is dat de juiste informatie, op de juiste plaats op de juiste tijd beschikbaar is.*

## Waar willen we naartoe?

---

Waar het om gaat is dat U op verschillende niveaus noodzakelijke en actuele veiligheidsinformatie deelt met elkaar. Daarover moeten de verschillende partijen met elkaar afspraken maken en deze afspraken vertalen in de eigen informatievoorziening. IBV biedt daarbij een referentiekader, dat het maken van afspraken en het uitvoeren daarvan vergemakkelijkt. IBV maakt inzichtelijk hoe de onderliggende structuur binnen de informatievoorziening eruit ziet. En dit allemaal om bij te dragen aan dat slagvaardige veiligheidsveld.

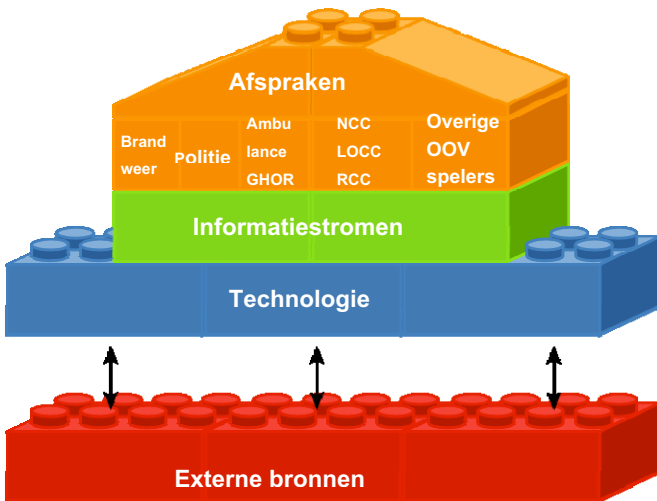
Er is een veelheid aan activiteiten over informatievoorziening. De situatie waar we naartoe willen is dat deze activiteiten op elkaar aansluiten, iedereen het kan gebruiken en het simpel uitbreidbaar is. Uiteindelijk gaat het om de vraag of iedereen op tijd de relevante informatie heeft om effectief te op te kunnen treden. Het is dus de bedoeling dat U zoveel mogelijk gebruik maakt van bestaande voorzieningen of ontwikkelingen die al in het veld spelen. Uw bedrijfsprocessen zijn zo vorm gegeven dat het meeste profijt wordt





getrokken uit de nieuwe mogelijkheden die de techniek biedt. Het geheel is modulair ingericht, zodat vernieuwingen op korte termijn zijn aan te brengen door één of meer kleine modules aan te passen of toe te voegen.

Hiermee kunnen we met kleine “slimme” bouwstenen komen tot een groot geheel. De afbeelding hieronder toont de samenhang van de functionaliteiten, technologie, informatiesystemen en informatieproducten en de daarvoor nodige afspraken met betrokken actoren. Zo ontstaat een logisch geheel.



Toelichting:

1. Het blauwe deel de fundering van het huis (technologie) is spraak, netwerken(infrastructuur) en koppelingen.
2. Het groene deel geeft de functionaliteiten, informatiesystemen en informatieproducten weer.
3. Het oranje deel de participanten binnen het OOV domein met de afspraken (governance)
4. De pijlen naar het rode deel is de connectie naar o.a basisregisters en overige systemen waaruit informatie wordt gewenst.

### ***De Chief Information Officer (CIO) kan u daar bij helpen***

De bestuurlijk portefeuillehouders informatievoorziening binnen de Veiligheidsregio's zien er op toe dat binnen de Veiligheidsregio de informatievoorziening op orde is.

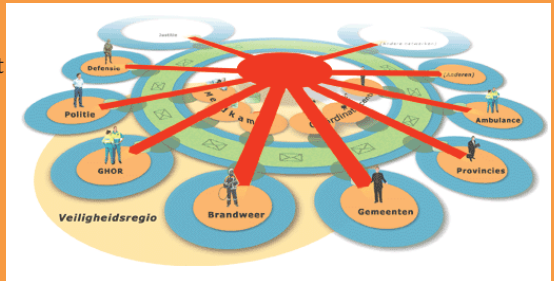
Om dit te bereiken kan het helpen een Chief Information Officer (CIO) binnen uw regio aan te stellen die opereert als linking pin tussen bestuur en uitvoering. De CIO kan het IBV gebruiken om een informatiebeleidsplan op te stellen. De interregionale samenwerking tussen CIO's verdient ook aandacht. Deze interregionale samenwerking zal uiteindelijk een eenduidige vraagarticulatie kunnen opleveren.

# Voorbeelden van lopende activiteiten en ontwikkelingen in beeld

## Netcentrisch Werken (NEC)

Het netcentrisch werken is oorspronkelijk afkomstig uit de Defensiewereld. Hier heeft het tot doel om zo efficiënt en effectief mogelijk te kunnen opereren in wisselende coalities op wisselende

plaatsen en onder wisselende omstandigheden. Ook in de rampenbestrijding wordt deze manier van werken gebruikt. De werkwijze vereist goede afspraken tussen de deelnemende ketenpartijen over het hebben en delen van informatie; de oranje verbindingslijnen in de IBV Galaxy.



## Informatiearchitectuur Sector Veiligheid (IASV)

Het IASV-project van de Raad-MIV zet op een rij bij welke activiteiten, welke specifieke informatie tussen veiligheidspartners wordt uitgewisseld. De IASV beschrijft wat de minimale inhoud van deze informatie is en wie betrokken zijn. Zo wordt inhoudelijk invulling gegeven aan de informatielaag van het IBV-model en wordt een landelijk uniform kader voor de informatie uitwisseling gerealiseerd. Voor meer informatie kunt u kijken op [www.raadmiv.nl](http://www.raadmiv.nl).





## Wat kunt u van BZK verwachten?

---

Om de IBV doelen te realiseren en daarmee het presterend vermogen van de veiligheidspartner te vergroten is het belangrijk dat we gezamenlijk dezelfde richting op gaan. BZK vindt het belangrijk om aan te geven waar we met zijn allen naartoe werken, maar kan en wil dit niet alleen.

Om dit te ondersteunen ontwikkelt BZK samen met de veiligheidspartners IBV-principes. Het Ministerie wil via deze principes richting geven aan de informatie-uitwisseling in de sector Veiligheid en de inrichting ervan beïnvloeden zonder zich met technische details te bemoeien. Deze principes zijn bedoeld als leidraad voor de inrichting van informatie-uitwisseling. Zij kunnen u helpen bij het inrichten van uw informatievoorziening.

Verder maakt BZK samen met u afspraken en zorgen wij er gezamenlijk voor dat standaarden worden vastgesteld. Tenslotte financiert het ministerie veelbelovende initiatieven die vallen binnen de IBV principes.

## Waar kunt u terecht?

---

Wilt u meer weten over IBV. Of heeft u een idee over verbetering van de informatievoorziening voor de veiligheidssector? U kunt terecht bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Op de website [www.minbzk.nl/onderwerpen/veiligheid/informatie-innovatie](http://www.minbzk.nl/onderwerpen/veiligheid/informatie-innovatie).

Voor vragen, brochures en posters kunt u bellen naar het programma Veiligheid, Informatie en Technologie (VIT) van het directoraat generaal Veiligheid op nummer 070-426 8557.

Februari 2009



*Bron: Maarten van der Voorde-Fotografie*

